Rishabh Ranjan

858-405-1419 riranjan@ucsd.edu linkedin.com/in/ranjan-rishabh github.com/ranjan-rishabh

Education

University of California, San Diego **Sep. 2021 – June 2026**
Doctor of Philosophy in Computer Science (Advised by Prof. Mihir Bellare) *3.97/4.0*

University of California, San Diego **Sep. 2021 – June 2023**
Masters of Science in Computer Science *3.97/4.0*

Birla Institute of Technology, Mesra **July 2015 – June 2019**
Bachelors of Engineering in Computer Science and Engineering *8.41/10*

Experience

Seagate Technology **June 2024 – Sept 2024**
Cryptography Research Intern *Shakopee, MN*

- Developed and analysed security of secure computation protocol based on Fully Homomorphic Encryption and Zero-Knowledge Proofs.

Microsoft **July 2019 – Sep. 2021**
Software Engineer *Bangalore, India*

- Designed and developed features for multiple Azure extensions as part of the Azure Storage team.
- Owner of multiple areas such as 'ordering' and 'virtual machines' in the Azure Stack Edge extension.
- Founding developer of the new Edge Ordering extension. Now generally available and being used by multiple teams in Azure and beyond.
- Automated deployment of microservices to ServiceFabric clusters saving developer time in each release cycle.
- Technologies: *Node, Typescript/JavaScript, C#, ReactJS, KnockoutJS, Redux*

Microsoft **May 2018 – July 2018**
Software Engineering Intern *Hyderabad, India*

- Created a Visual Studio extension based on syntax parsing and compilation to provide real time warnings about accessibility violations in code. Received Pre-Placement Offer for this.
- Alleviated the need for accessibility testing as a stage in development and saved hundreds of developer hours.
- Technologies: *C#, Managed Extensibility Framework, Roslyn (compiler platform for Visual Studio)*

Publications

- Rishabh Ranjan, Dr. Vathsala H, Dr Shashidhar G Koolagudi (2021), *Profile Generation from Web Sources: An Information Extraction System*, Soc. Netw. Anal. Min. (Springer) 12, 2 (2022). DOI
- Dr. Itu Snigdh, Shashank Srigiri, Rishabh Ranjan (2018), *Scheduling sensor nodes for enhancing energy savings in a Wireless sensor network*, Journal of Network and Information Security. ISSN 2321-685

Technical Skills

Languages: C, C++, Python, JavaScript, TypeScript, C#, WebAssembly, SQL
Frameworks: OpenFHE, Tensorflow, PyTorch, CUDA, BOOST, MySql, mlpack, MPI
Areas: Provable security, Multi-party computation, Post-quantum cryptography

Projects

Verifiable Homomorphic Encryption using CF13 | *C++, MAC* **March 2023**

- Implemented the CF13 homomorphic MAC described in the paper titled, *Practical Homomorphic MACs for Arithmetic Circuits* by Dario Catalano and Dario Fiore (Eurocrypt, 2013).

Faster Matrix Multiplication | *CUDA, C++, GPU architecture* **October 2022**

- Optimization of large Matrix multiplication using CUDA on a Turing GPU
- The project utilized multi-threading along with instruction level parallelism to induce higher computational intensity.

Python to WebAssembly Compiler | *WebAssembly, Typescript, Python, Compiler Optimizations* **May 2022**

- Created a compiler as a group class project for compiling Python programs to WebAssembly which can be executed using Javascript on the browser.
- Worked on compiler optimizations such as constant folding and propagation, copy propagation, dead code elimination, hoisting using Worklist infrastructure, structured control flow using stackifier algorithm.

γ^2-SVP to γ-HSVP reduction | *Python, Lattices, Fplll* **December 2021**

- Gave and implemented the γ^2-Shortest vector problem (SVP) to γ-Hermite shortest vector problem in lattices. The idea of reduction is described in the paper *An algorithmic theory of numbers, graphs and convexity.* by Laszlo Lovasz.
- This project fills the gap in reduction and gives an implementation of the reduction.

Meeting notes extraction and summarization in MS Teams | *Azure Cognitive Services, Python* **July 2020**

- Make transcripts from recorded meetings and provide a summary of the meeting along with meeting notes in Microsoft Teams.

Teaching Assistant Experience

- CSE107: Introduction to Modern Cryptography — UCSD | *Spring 21, 23, Fall 22, Winter 22, Spring 24*
- CSE101: Design and Analysis of Algorithms — UCSD | *Summer 22*
- CSE105: Theory of Computation — UCSD | *Fall 21*

Graduate Courses

- **Cryptography** : Lattice Algorithms, Modern Cryptography, Applied Cryptography, Advanced Cryptography (FHE), Quantum Cryptography
- **Complexity theory** : Computability and Complexity, Analysis of Algorithms, Semi-definite Programming
- **Systems** : Advanced Compiler Design, Parallel and Distributed Computing